UNITED STATES DISTRICT COURT FOR THE

MIDDLE DISTRICT OF TENNESSEE

THROUGH THE FOREST COUNSELING INC., individually and on behalf of all others similarly situated, Plaintiff, v. CHANGE HEALTHCARE INC. and UNITEDHEALTH GROUP INCORPORATED, Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Through the Forest Counseling Inc. ("Plaintiff"), individually and on behalf of the Class defined below, brings this action against Defendants Change Healthcare Inc. ("Change Healthcare") and UnitedHealth Group Incorporated ("UnitedHealth") and alleges as follows:

INTRODUCTION

1. This action arises out of Defendants' failure to maintain secure data security systems. On February 22, 2024, UnitedHealth announced that it had experienced a cybersecurity incident (the "Data Breach"). UnitedHealth also disclosed that the incident affected its subsidiary, Defendant Change Healthcare. The attack has had devastating consequences nationwide for medical businesses like Plaintiff's.

2. Change Healthcare—a healthcare technology company—processes 15 billion health care transactions annually, including for service that directly affect patient care and pharmacy operations. The Data Breach had an immediate and lasting adverse impact on patient

care services, claims processing, and revenue cycle management, among other things. Providers like Plaintiff were unable to process payment for their services, resulting in cash flow shortages and significant operational challenges and administrative burdens.

3. Plaintiff and Class members now must contend with the indefinite, continuing fallout from the Data Breach. Plaintiff therefore brings this action for damages or restitution, as well as injunctive relief, on its own behalf and for all others similarly situated.

PARTIES

4. Plaintiff Through the Forest Counseling Inc. is a Massachusetts corporation with a principal place of business in Boston, Massachusetts.

5. Defendant Change Healthcare Inc. is a Delaware corporation with its principal place of business in Nashville, Tennessee.

6. Defendant UnitedHealth Group, Inc. is a Delaware corporation with its principal place of business in Minnetonka, Minnesota.

JURISDICTION AND VENUE

7. This Court has jurisdiction over the lawsuit under the Class Action Fairness Act, 28 U.S.C. § 1332, because this is a proposed class action in which: (1) there are at least 100 class members; (2) the combined claims of class members exceed $5,000,000, exclusive of interest, attorneys' fees, and costs; and (3) Defendants and one or more class members are citizens of different states.

8. The Court has personal jurisdiction over Change Healthcare because its principal place of business is within this District, and it has sufficient minimum contacts in Tennessee to render the exercise of jurisdiction by this Court proper and necessary. The Court also has personal jurisdiction over UnitedHealth Group, Inc. because it purposefully avails itself of the

benefits and protections of this state by conducting business in Tennessee, and in so doing, maintains sufficient minimum contacts in Tennessee to render the exercise of jurisdiction by this Court proper and necessary.

9. For the same reasons, venue is properly laid in this forum under 28 U.S.C. § 1391(b).

FACTUAL ALLEGATIONS

A. Background Regarding Change Healthcare

10. Change Healthcare—a subsidiary of UnitedHealth—is a healthcare technology company that describes itself as a provider of "industry-leading analytics, expansive data, and unparalleled connection and data transfer between providers, payers, and consumers, to help improve workflows, increase administrative and financial efficiencies, and improve clinical decisions."

11. Change Healthcare provides payment processing services, acting as middleman between the health care provider and the health insurer. It processes billions of transactions every year for more than 340,000 physicians and 60,000 pharmacies.

12. Before it was acquired by Defendant UnitedHealth in late 2022, Change operated as a standalone company. UnitedHealth is a vertically integrated healthcare enterprise that owns one of the largest health insurers in the United States, UnitedHealthcare; one of the largest PBMs in the United States, OptumRX; a large provider network, OptumHealth; and a healthcare technology business, among other businesses. Because of the potential anticompetitive effects of UnitedHealth's acquisition of Change Healthcare, the DOJ sued to enjoin the transaction in February 2022.

13. The DOJ noted in part that Change operates as the "leading independent supplier of technologies used by healthcare providers to submit health insurance claims, and by health insurance companies to evaluate and process these claims." The DOJ further alleged that—in connection with its services—Change operates an electronic data interchange "clearinghouse, which transmits data between healthcare providers and insurers, allowing them to exchange insurance claims, remittances, and other healthcare-related transactions." The data included in the clearinghouse shows the treatment individuals receive, the coverage they have, and how that coverage operates to pay for healthcare procedures.

14. According to the DOJ, United's acquisition of Change "would fundamentally alter the health insurance industry," as "United would gain unprecedented access to a vast trove of its health insurance rivals' competitively sensitive claims data[.]"

15. UnitedHealth's data and Change's data also would be concentrated under one roof, presenting a broad scale, highly attractive target for cyberattackers.

16. The DOJ ultimately withdrew its challenge to the UnitedHealth-Change Healthcare merger, which closed in October 2023.

17. With respect to the security of the data held on its systems, Change Healthcare acknowledges that "[p]rivacy matters," and states that it "follow[s] a privacy framework that helps us to manage and protect your personal information in the products and services we provide[.]"

18. With respect to data security, Change Healthcare represents in its Privacy Notice:

> We implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse. These measures are aimed at providing on-going integrity and confidentiality of data, including your personal information. We evaluate and update these measures on an ongoing basis.

B. The Data Breach

19. Defendant UnitedHealth disclosed the Data Breach in a filing with the Securities and Exchange Commission on February 22, 2024. UnitedHealth stated:

> On February 21, 2024, UnitedHealth Group (the "Company") identified a suspected nation-state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems. Immediately upon detection of this outside threat, the Company proactively isolated the impacted systems from other connecting systems in the interest of protecting our partners and patients, to contain, assess and remediate the incident.
>
> The Company is working diligently to restore those systems and resume normal operations as soon as possible, but cannot estimate the duration or extent of the disruption at this time. The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies. At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational.
>
> During the disruption, certain networks and transactional services may not be accessible. The Company is providing updates on the incident . . . .
>
> As of the date of this report, the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition or results of operations.

20. The Data Breach has had debilitating effects on the United States healthcare system, including providers like Plaintiff, which have been unable to timely collect billions of dollars in payments. The Data Breach forced Defendants to shut down parts of Change Healthcare's systems, depriving a large number of providers of the ability to obtain insurance approval for their services—meaning they could not get paid. More than a month after the breach, certain health care providers have still been unable to collect payment for services rendered.

21. As providers incur late-payment penalties and struggle to keep up with payroll, rent, and overhead, many have been forced to dip into personal funds, and many are incurring extra administrative expenses to perform the services previously handled by Change Healthcare. Pharmacies have been unable to fill prescriptions, access to care has been disrupted, and the American healthcare system has been substantially burdened as a result of the attack.

22. As the American Hospital Association noted, "the Change Healthcare cyberattack is the most significant and consequential incident of its kind against the U.S. health care system in history" and "has made it harder for hospitals to provide patient care, fill prescriptions, submit insurance claims, and receive payment for the essential health care services they provide."

23. Although UnitedHealthcare initially attributed the Data Breach to a "nation-state," the hacking group BlackCat claimed responsibility. In doing so, it disclosed that it had exfiltrated the personal information of millions of Americans. According to BlackCat:

> UnitedHealth has announced that the attack is 'strictly related' to Change Healthcare only and it was initially attributed to a nation-state actor. Two lies in one sentence.
>
> . . .
>
> Only after threatening them to announce it was us, they started telling a different story.
>
> . . .
>
> It is true that the attack is centered at Change Healthcare [production] and corporate networks, but why is the damage extremely high?
>
> . . .
>
> Change Healthcare production servers process extremely sensitive data to all of UnitedHealth clients that rely on Change Healthcare technology solutions, meaning thousands of healthcare providers, insurance providers, pharmacies, etc …
>
> . . .
>
> Also, being inside a production network, one can imagine the amount of critical and sensitive data that can be found.

24. BlackCat stated it had exfiltrated six terabytes of data affecting Medicare, Tricare, CVS CareMark, Loomis, Davis Vision, Health-Net, MetLife, Teachers Health Trust, and other significant U.S. healthcare entities. BlackCat further stated the data includes "millions" of medical and other sensitive records, claims information, insurance records, and personally identifiable information ("PII") of patients, including active military personnel.

25. On March 13, 2024, the United States Department of Health and Human Services' Office for Civil Rights ("OCR")—the federal government office responsible for enforcing the HIPAA Privacy, Security, and Breach Notification rules—issued a "Dear Colleague" letter addressing the Change Healthcare Data Breach. OCR stated, among other things, that it was:

> [A]ware that Change Healthcare, a unit of UnitedHealth Group (UHG), was impacted by a cybersecurity incident in late February that is disrupting health care and billing information systems nationwide. The incident poses a direct threat to critically needed patient care and essential operations of the health care industry.
>
> . . .
>
> Given the unprecedented magnitude of this cyberattack, and in the best interest of patients and health care providers, OCR is initiating an investigation into this incident. OCR's investigation of Change Healthcare and UHG will focus on whether a breach of protected health information occurred and Change Healthcare's and UHG's compliance with the HIPAA Rules.

C. Defendants Had a Duty to Maintain Adequate Cybersecurity Systems and Protocols

26. Defendants are entities covered by HIPAA (*see* 54 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information").

27. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[1] Moreover, HIPAA requires that Defendants implement appropriate safeguards for this confidential information.[2]

28. Similarly, HIPPA requires that Defendants:

- Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights, *see* 45 C.F.R. § 164.312(a)(1);
- Implement policies and procedures to prevent, detect, contain, and correct security violations, *see* 45 C.F.R. § 164.306(a)(1);
- Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, *see* 45 C.F.R. § 164.306(a)(2);
- Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, *see* 45 C.F.R. § 164.306(a)(3);
- Ensure compliance with the HIPAA security standard rules by its workforce, *see* 45 C.F.R. § 164.306(a)(4); and
- Effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information, *see* 45 C.F.R. § 164.530(b).

[1] 45 C.F.R. § 164.502 (2009).
[2] 45 C.F.R. § 164.530(c)(1) (2009).

29. Defendants knew that they maintained sensitive data on their systems and that they faced a heightened risk of cyberattack due to the nature of that data.

30. The healthcare industry is an attractive target for cyberattackers and other criminal actors on the "dark web" black market. According to the *New York Times*, medical records command multiple times the amount of money that a stolen credit card commands on the dark web, in part because medical information—unlike credit card information—cannot be easily changed. According to John Riggi, of the American Hospital Association, medical records are valuable to malicious actors "because it's easy to commit health care fraud."

31. Federal and state government bodies have established security standards and issued recommendations to reduce the risk of cyberattack and the resulting harm to consumers and institutions. The Federal Trade Commissions has issued numerous guidelines for businesses highlighting the importance of robust and effective data and cyber security practices. The FTC has advised that it is imperative that companies factor data and cyber security into all business decision-making.

32. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established guidelines for fundamental data and cyber security principles and practices for business. The guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines further recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the

system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

33. The FTC also advises that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

34. The FTC has brought enforcement actions against businesses for failing to adequately protect confidential consumer data, treating the failure to employ appropriate measures to prevent unauthorized access to such data as an unfair practice that violates Section 5 of the FTC Act, 15 U.S.C. § 45(a).

D. Plaintiff-Specific Allegations

35. Through the Forest Counseling Inc. is a full-service psychotherapy practice based in Boston, Massachusetts.

36. Plaintiff used Change Healthcare for its payment processing services.

37. Plaintiff, directly or indirectly, submits insurance claims to Change Healthcare for payment. The claims are directed to the relevant insurer, and, once approved, Plaintiff is paid.

38. Since the Data Breach, Plaintiff has not received payment for a large portion of its services. As a result, Plaintiff has not received thousands of dollars in reimbursement it is owed. Nor has Plaintiff been provided with any timeline for reimbursement.

39. Because of the Data Breach and inability to obtain payment for services rendered, Felicha Laforest, the founder and head of Through the Forest Counseling Inc., has been forced to incur additional administrative expense, including in attempting to manually perform the payment processing services for which Change Healthcare is generally responsible, being forced

to pay business expenses using personal funds, and expending considerable time and effort addressing the consequences of Defendants' failure to provide payment processing and other services.

40. Despite directly or indirectly paying for Change Healthcare's services, Plaintiff has been denied access to them, resulting in ongoing damage.

CLASS ACTION ALLEGATIONS

41. Plaintiff brings this class action on behalf of itself and all others similarly situated pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and where applicable, 23(c)(4), on behalf of the following Class: All healthcare providers in the United States who, from the time of the Data Breach to present, used or attempted to use Change Healthcare's services.

42. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

43. Plaintiff reserves its right to modify the Class definition, including based on discovery and further investigation.

44. The Class is so large as to make joinder impracticable. There are at least hundreds of Class members. Disposition of their claims in a single action will provide substantial benefits to all parties and to the Court. Class members are readily ascertainable from information and records in Defendants' possession, custody, or control.

45. Plaintiff's claims are typical of the claims of the Class, as Plaintiff, like all Class members, experienced disruption in Change Healthcare's services as a result of the Data Breach.

46. Plaintiff is a member of the Class and will fairly and adequately represent and protect its interests. Plaintiff's counsel is competent and experienced in prosecuting class actions, including relating to data breaches. Plaintiff has no interest contrary to or in conflict with the interests of any other Class member.

47. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual Class members. Among the questions of law and fact common to the Class are:

- Whether Defendants engaged in the conduct alleged;
- Whether Defendants had a duty to implement reasonable cyber security measures to protect against cyberattack;
- Whether Defendants breached that duty by failing to take reasonable precautions to protect against cyberattack;
- Whether Change Healthcare breached agreements with Plaintiff and Class members by failing to provide its payment processing and other services;
- Whether Plaintiff and Class members are entitled to damages or restitution and in what amount; and
- Whether Plaintiff and Class members are entitled to entry of appropriate injunctive relief against Defendants.

48. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would have no effective remedy. Given the relatively small size of the individual Class members' claims, few, if any, Class members would

seek redress for Defendants' violations individually. Class treatment will conserve the resources of the courts and promote consistency and efficiency of adjudication.

49. Defendants acted or refused to act on grounds generally applicable to the Class, making injunctive and corresponding declarative relief appropriate with respect to the Class as a whole.

50. Class certification also is appropriate under Rules 23(b)(1) and/or (c)(4) because:

- The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendants.
- The prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests.
- The claims of Class members are comprised of common issues whose resolution in a class trial would materially advance this litigation.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)
(Against all Defendants)

51. Plaintiff incorporates and realleges the foregoing allegations of fact.

52. Defendants collected sensitive information from Plaintiff and Class members in connection with Defendants' payment processing and other services. Defendants undertook to perform integral payment processing and other services, on which Plaintiff and Class members' businesses depended.

53. Defendants owed Plaintiff and Class members a duty of reasonable care to preserve and protect the information being stored, transferred, and secured and to ensure that Defendants' payment processing and other services stayed operational and did not experience extended outages or unavailability.

54. This duty included, among other obligations, maintaining and testing Defendants' security systems and computer networks, implementing training and other protocols and procedures to guard against cyberattack, and taking other reasonable security measures to safeguard and adequately secure its systems from unauthorized access and use.

55. Defendants' duty further included the obligation to provide data security consistent with industry standards and other requirements discussed herein, and to ensure Defendants' electronic systems and networks were adequately protected at all relevant times.

56. Defendants had a common law duty to prevent foreseeable harm to others, including their customers. Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. It was foreseeable that Plaintiffs and Class members would be harmed by Defendants' failure to protect against cyberattack. Defendants knew that hackers routinely target medical information like that housed on Defendants' systems, and Defendant knew that such an attack would or could freeze or otherwise impair services Defendants were providing to Plaintiff and Class members, on which they rely.

57. Defendants also owed a duty to Plaintiff and Class members, by operation of statute, to implement and ensure adequate data security practices. For instance, under the FTC Act, 15 U.S.C. § 45(a), Defendants had a duty to provide fair and adequate computer systems and data security practices, including to safeguard PII.

58. Defendants' actions and inaction breached its duties by failing to provide adequate data security to safeguard its systems.

59. Defendants' breaches constitute negligence and negligence per se.

60. Plaintiff and Class members were the foreseeable victims of Defendants' inadequate and ineffectual cybersecurity. The natural and probable consequence of Defendants' failure to adequately secure its information networks was a disruption in the services upon which Defendants knew Plaintiff and Class members rely.

61. Defendants knew they were an attractive target for cyber thieves, particularly in light of data breaches experienced by other entities around the United States. The Data Breach was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches.

62. There is a close connection between Defendants' failure to employ reasonable security protections for its systems and the injuries suffered by Plaintiff and Class members. Defendants' vulnerability to cyberattack resulted in its systems being taken down, and the inability of Plaintiff and Class members to process payments through those systems.

63. The policy of preventing future harm disfavors application of the economic loss rule, particularly given the sensitivity of the private information entrusted to Defendants. A high degree of opprobrium attaches to Defendants' failure to secure their systems. Defendants had an independent duty in tort to protect this information and thereby avoid reasonably foreseeable harm to Plaintiff and Class members.

64. As a result of Defendants' negligence, Plaintiff and Class members have suffered actual damages in an amount to be proven at trial. Plaintiff and Class members seek an award of nominal damages in the alternative.

SECOND CAUSE OF ACTION
BREACH OF CONTRACT (THIRD-PARTY BENEFICIARY)
(On Behalf of Plaintiff and the Class)
(Against Change Healthcare)

65. Plaintiff incorporates and realleges the foregoing allegations of fact.

66. Change Healthcare contracted with various businesses to provide payment processing and other services for the ultimate benefit of Plaintiff and Class members.

67. Change Healthcare and these entities intended that Plaintiff and Class members benefit from Change Healthcare's payment processing services.

68. Plaintiff submits insurance claims for payment through Change Healthcare, which Change Healthcare, in turn, submits to insurance companies for payment.

69. Plaintiff, directly or indirectly, paid for Change Healthcare's services and discharged any and all other duties that Plaintiff owed.

70. In exchange, Change Healthcare was to provide its payment processing and other services.

71. In February 2024, after the Data Breach, Change Healthcare deactivated its payment processing and other services, severing Plaintiff's and Class members' access to and ability to use those services, in breach of Change Healthcare's contractual obligations.

72. As a direct and proximate result of Change Healthcare's breaches, Plaintiff and Class members sustained actual losses and damages in an amount to be proven at trial. Plaintiff and Class members seek an award of nominal damages in the alternative.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)
(Against Change Healthcare)

73. Plaintiff incorporates and realleges the foregoing allegations of fact.

74. Plaintiff brings this count in the alternative to its legal claims and lacks an adequate remedy at law.

75. Plaintiff and Class members conferred a benefit on Change Healthcare by paying it money for services rendered.

76. Change Healthcare appreciated and had knowledge of the benefits conferred upon it by Plaintiff and Class members.

77. In exchange for receiving Plaintiff's and Class members' money, which provided Change Healthcare a commercial benefit, Change Healthcare was obligated to supply Plaintiff and Class members with access to and use of its payment processing and other services. Following the Data Breach, however, Change Healthcare deactivated those services.

78. Equity and good conscience forbid retention by Change Healthcare of the financial benefits it obtained from Plaintiff and Class members under these circumstances.

79. As a result of Change Healthcare's wrongful conduct, Plaintiff and Class members suffered harm as described herein and are entitled to restitution. Change Healthcare should therefore be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds it received therefrom.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for an order:

A. Certifying this action as a class action, appointing Plaintiff as a Class representative, and appointing Plaintiff's counsel to represent the Class;

B. Entering judgment for Plaintiff and the Class;

C. Awarding Plaintiff and Class members actual or nominal damages or restitution;

D. Ordering appropriate injunctive relief;

E. Awarding pre- and post-judgment interest as prescribed by law;

F. Awarding reasonable attorneys' fees and costs as permitted by law;

G. Granting such further and other relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED: April 1, 2024

/s/ Jerry E. Martin
Jerry E. Martin (TNBPR No. 20193)
Seth M. Hyatt (TNBPR No. 31171)
Matthew E. McGraw (TNBPR No. 032257)
BARRETT JOHNSTON MARTIN & GARRISON, PLLC
200 31st Ave. N
Nashville, TN 37203
(615) 244-2202
jmartin@barrettjohnston.com
shyatt@barrettjohnston.com
mmcgraw@barrettjohnston.com

Adam E. Polk (CA State Bar No. 273000)*
Jordan Elias (CA State Bar No. 228731)*
GIRARD SHARP LLP
apolk@girardsharp.com
jelias@girardsharp.com
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

Attorneys for Plaintiffs

*Pro Hac Vice forthcoming